State of Utah

DEPARTMENT OF COMMERCE
DIVISION OF CONSUMER PROTECTION
Heber M. Wells Building
160 East 300 South
PO Box 146704
Salt Lake City, UT 84114
801-530-6601

PRESS RELEASE
Date: 21 October 2000

Contact Person: Francine Giani, Director
Telephone: 801-530-6601

What Can Consumers Do To Avoid Becoming Victims of Identity Fraud?

Identity fraud is on the rise. Often the first notice consumers get that someone has fraudulently assumed their identity is either a call from a collection agency demanding payment on an overdue credit account which they never opened or when their own monthly billing statements do not arrive in the mail and they find out the address on their account has been changed by an identity thief. Most victims never learn how the identity thieves accessed their personal identifying information.

Indeed, it may be impossible for a consumer to prevent access to all his or her personal information which is so readily available to thieves (and to junk marketers) from a variety of sources. While the following recommendations won't prevent fraud entirely, consumers can take these preventative steps to close some avenues of identity fraud.

PROTECT PERSONAL INFORMATION

Always question the information gathering and handling practices of merchants, financial institutions, creditors, government agencies, employers, educational institutions and others . . . ask, do they really need this information for a valid purpose?

Credit card account numbers--never provide any personal, bank account or credit card information to anyone who contacts you through a telephone solicitation. Instead, it is advisable to demand they mail you information so that you can further research the company and their products and services.

Keep items with personal information in a safe place. Keep a list of all credit cards, account numbers, expiration dates, and the customer service phone numbers in a secure place so that you can quickly contact your creditors in case your cards are lost or stolen.

Tear Up/Destroy all ATM and bank receipts, old insurance forms, bank checks, expired credit cards, and any other papers that include personal information, identification, and account numbers about you. This includes pre-approved credit card solicitations! Thieves oftentimes search through your garbage to find these forms and information and use it to apply for credit in your name.

Minimize the number of credit cards and other items with personal information printed on them that you carry. Cancel all inactive accounts. Even though you do not use them, those accounts appear on your credit report, which can be used by thieves.

Do not leave envelopes containing your checks in your home mailbox, unless it's secured. Due to the increased risk of theft, it is best to mail bills and other sensitive items at the post office, rather than from your residence.

When creating passwords or PINs, do not use the last four digits of your Social Security Number, your birth date, middle name, mother's maiden name, address or anything else that could be discovered easily by thieves.

Social security numbers--ask to have an alternative number where social security numbers are used for identification by schools, employers, or other institutions; resist writing your social security number on checks where possible, keep tax records and other financial documents in a secure place and destroy or delete social security numbers from any documents before throwing them away.

Address and phone number--do not give out or write your name and address down in conjunction with a credit card sale. You may want to have your name, address, and phone number deleted from marketers' lists by writing to Direct Marketing Associations Mail Preference Service (P.O. Box 9008, Farmingdale, NY 11735) and Telephone Preference Service (P.O. Box 9015, Farmingdale, NY 11735).

Other common identifying information--consider using other security passwords for financial accounts rather than common identifiers such as mother's maiden name and birth date; if you have your driver's license pre-printed on your checks, always shred canceled checks before throwing away.

MONITOR CREDIT REPORTS

Obtain a copy of your credit report on a regular basis to monitor for changed addresses and fraudulent account information.

MONITOR BILLING STATEMENTS

Check your billing statements each month for fraudulent charges and report immediately. If you do not receive your statement on time, it may be that a fraudulent change of address was sent to the creditor or the post office. Call the creditor first and then the post office to see if a change of address has been filed in your name.

PRE-APPROVED CREDIT CARD OFFERS

"Credit card: 6% APR!!" These brightly-colored gimmicks from banks are easily converted to fraudulent accounts. Always tear up pre-approved credit card applications before throwing them away. Credit card solicitations are generated from "pre-screened lists" of credit reports provided by credit bureaus. If you do not want to receive these offers, contact each of the Big Three credit bureaus to remove your name from pre-screened lists.